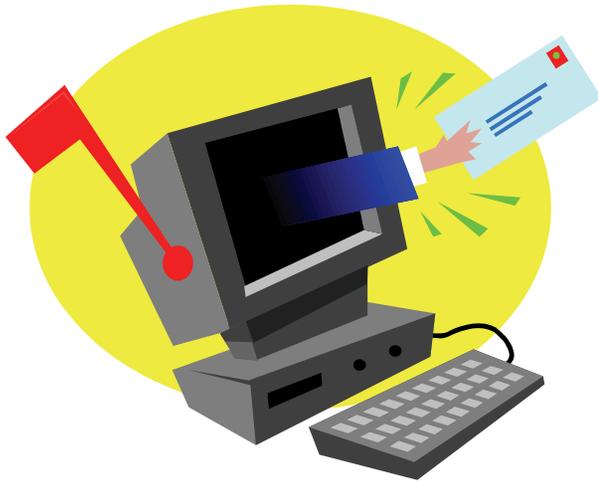


# JULY 2007

**W**hile e-mail attachments are a popular and convenient way to send documents, they are also a common source of viruses. E-mail programs try to

address all users' needs. Almost any type of file can be attached to an e-mail message, so attackers have freedom with the types of viruses they can send. Use caution when opening attachments, even if they appear to have been sent by someone you know.

Just because an e-mail message looks like it came from your mom, grandma or boss doesn't mean that it did. Many viruses can "spoof" the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This includes e-mail messages that appear to be from your Internet service provider (ISP) or software vendor that claim to include patches or anti-virus software. ISPs and software vendors do not send patches or software in e-mail. 



Sun	Mon	Tue	Wed	Thu	Fri	Sat	
1	2	3	 4 State Holiday	5	6  Pay Day	7	
8	9	10	11	12	13	14	
15	16	17	18	19	20  Pay Day	21	
22	23	24	25	26	27	28	
29	30	31	 <i>ADOA Information Security</i> <b>AIS</b> Managing Our Information Safeguards				E-mail: <a href="mailto:ADOA.InfoSec@azdoa.gov">ADOA.InfoSec@azdoa.gov</a> Phone: 602-542-2252 <a href="http://www.azdoa.gov/isd/ais">http://www.azdoa.gov/isd/ais</a>